ISSN 2181-3187

MIJOZ ILOVALARIGA HUJUM TURLARI.

Shaydullayev Jahongir Qudrat o‘g‘li

Muhammad al-Xorazmiy nomidagi

Toshkent axborot texnologiyalari universiteti

Shaydullayevjahongir579@gmail.com

Annotatsiya: *Mazkur tezisda zamonaviy kiberxavfsizlik tahdidlaridan biri bo‘lgan mijoz ilovalariga qarshi hujumlar turlari yoritilgan. Unda eng ko’p uchraydigan 10 ta hujum turi haqida batafsil ma’lumot berilgan: Phishing, DDoS, SQL Injection, Cross-Site Scripting (XSS), Man-in-the-Middle, Zero-Day, Ransomware, API hujumlari, Session Hijacking va Clickjacking. Har bir hujumning ishlash mexanizmi, maqsadi va qanday zaifliklardan foydalanishi misollar bilan tushuntirilgan. Tadqiqot mijoz ilovalari xavfsizligini ta’minlashda ehtiyotkorlik choralarini belgilash, foydalanuvchilarni xabardor qilish va dasturiy zaifliklarni bartaraf etish bo‘yicha muhim ahamiyatga ega.*

Аннотация: *В данной диссертации рассматриваются типы атак на клиентские приложения, которые являются одной из современных угроз кибербезопасности. В нем содержится подробная информация о 10 наиболее распространенных типах атак: фишинг, DDoS, SQL-инъекции, межсайтовый скриптинг (XSS), Man-in-the-Middle, нулевой день, программы-вымогатели, атаки API, перехват сеанса и кликджекинг. Механизм работы, цель и уязвимости, используемые каждой атакой, поясняются на примерах. Исследование важно для определения мер предосторожности, обеспечивающих безопасность клиентских приложений, информирования пользователей и устранения уязвимостей программного обеспечения.*

Abstract: *This thesis covers the types of attacks against client applications, which are one of the modern cybersecurity threats. It provides detailed information about the*

ISSN 2181-3187

10 most common types of attacks: Phishing, DDoS, SQL Injection, Cross-Site Scripting (XSS), Man-in-the-Middle, Zero-Day, Ransomware, API attacks, Session Hijacking, and Clickjacking. The mechanism of action, purpose, and vulnerabilities exploited by each attack are explained with examples. The study is important in determining precautions to ensure the security of client applications, informing users, and eliminating software vulnerabilities.

Kalit so'zlar: *Axborot xavfsizligi,Kiberhujumlar, Mijoz ilovalari,Fishing (Phishing), DDoS (Distributed Denial of Service), SQL Injection, XSS (Cross-Site Scripting), MITM (Man-in-the-Middle), Zero-Day zaiflik, Ransomware, API hujumlari, Sessiyani egallash (Session Hijacking), Clickjacking, Zaiflikdan foydalanish, Web xavfsizlik.*

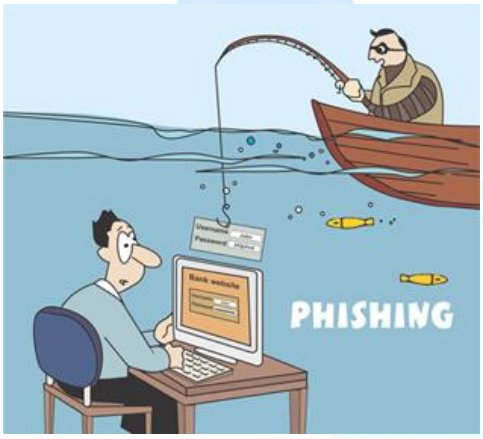
Ключевые слова: *Информационная безопасность, Кибератаки, Клиентские приложения, Фишинг, DDoS (Распределенный отказ в обслуживании), SQL-инъекция, XSS (Межсайтовый скриптинг), MITM (Человек посередине), Уязвимость нулевого дня, Программы-вымогатели, Атаки на API, Перехват сеанса, Clickjacking, Эксплуатация уязвимостей, Веб-безопасность.*

Keywords*: Information Security, Cyberattacks, Client Applications, Phishing, DDoS (Distributed Denial of Service), SQL Injection, XSS (Cross-Site Scripting), MITM (Man-in-the-Middle), Zero-Day Vulnerability, Ransomware, API Attacks, Session Hijacking, Clickjacking, Vulnerability Exploitation, Web Security.*

Mijoz ilovalariga qilingan hujumlar turli usullar orqali amalga oshiriladi. Quyida eng keng tarqalgan hujum turlari haqida qisqa ma'lumot berilgan:

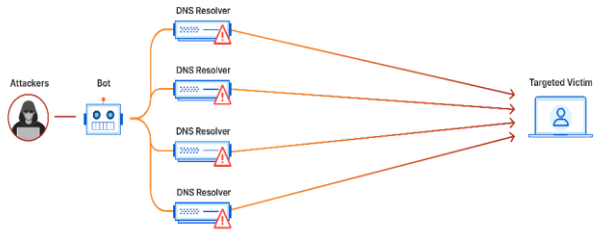
ISSN 2181-3187

1. Fishing (Phishing) - Foydalanuvchilarni aldash orqali ularning maxfiy ma’lumotlarini (login, parol, kredit karta ma’lumotlari) qo‘lga kiritish. Ko‘pincha soxta elektron pochta xabarlari yoki veb-saytlar orqali amalga oshiriladi.



Fishing ijtimoiy injeneriya va firibgarlikdir, bunda tajovuzkorlar odamlarni maxfiy ma'lumotlarni oshkor qilish yoki viruslar, qurtlar, reklama dasturlari yoki to'lov dasturlari kabi zararli dasturlarni o'rnatish uchun aldashadi. Fishing hujumlari tobora takomillashib bordi va ko'pincha nishonga olingan saytni shaffof aks ettiradi, bu esa tajovuzkorga jabrlanuvchi sayt bo'ylab harakatlanayotganda va jabrlanuvchi bilan qo'shimcha xavfsizlik chegaralarini kesib o'tayotganda hamma narsani kuzatish imkonini beradi. 2020 yil holatiga ko‘ra, bu kiberjinoyatlarning eng keng tarqalgan turi bo‘lib, FQBning Internetdagi jinoyatlar bo‘yicha shikoyat markazi har qanday kiberjinoyatga qaraganda ko‘proq fishing hodisalari haqida xabar beradi.

2. DDoS (Distributed Denial of Service) hujumi. Server yoki tarmoqqa ortiqcha so‘rovlar yuborish orqali ularni ishdan chiqarish. Bu hujum foydalanuvchilarning xizmatlardan foydalanishini qiyinlashtiradi.

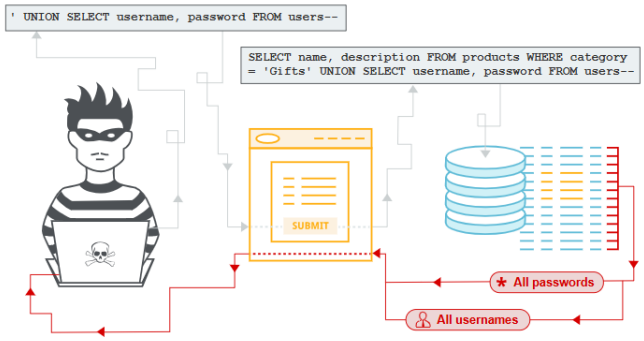


Hisoblashda xizmat ko‘rsatishni rad etish hujumi (DoS hujumi) bu kiberhujum bo‘lib, unda jinoyatchi tarmoqqa ulangan xost xizmatlarini vaqtincha yoki cheksiz muddatga to‘xtatib, mashina yoki tarmoq resursini o‘z mo‘ljallangan foydalanuvchilari uchun foydalana olmaydigan qilib qo‘yishga intiladi. Xizmat ko'rsatishni rad etish odatda tizimlarni ortiqcha yuklash va qonuniy so'rovlarning bir qismini yoki barchasini bajarishga yo'l qo'ymaslik uchun maqsadli mashina yoki resursni ortiqcha so'rovlar bilan to'ldirish orqali amalga oshiriladi. Hujumlar diapazoni juda xilma-xil bo'lib, uning ishlashini sekinlashtirish uchun millionlab so'rovlar bilan

ISSN 2181-3187

serverni to'ldirishdan tortib, katta miqdordagi yaroqsiz ma'lumotlarga ega bo'lgan serverni to'ldirishdan tortib, noqonuniy IP-manzil bilan so'rovlarni yuborishgacha bo'lgan. Taqsimlangan xizmatdan bosh tortish hujumida (DDoS hujumi) jabrlanuvchini suv bosadigan kiruvchi trafik turli manbalardan kelib chiqadi.

3. *SQL Injection.* Veb-ilovalardagi ma’lumotlar bazalariga noqonuniy SQL so‘rovlar yuborish orqali tizimdan maxfiy ma’lumotlarni olish yoki o‘zgartirish. Hisoblashda SQL injection - bu ma'lumotlarga asoslangan ilovalarga hujum qilish uchun ishlatiladigan kodni kiritish usuli bo'lib, unda zararli SQL bayonotlari bajarish uchun kirish maydoniga kiritiladi (masalan, ma'lumotlar bazasi tarkibini tajovuzkorga tashlash uchun).

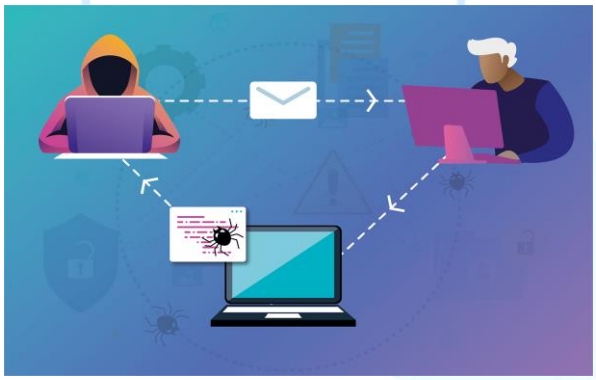


SQL in'ektsiyasi ilovaning dasturiy ta'minotidagi xavfsizlik zaifligidan foydalanishi kerak, masalan, foydalanuvchi kiritgan ma'lumotlar SQL bayonotlariga o'rnatilgan satrning literal qochish belgilari uchun noto'g'ri filtrlanganda yoki foydalanuvchi kiritgan ma'lumotlar kuchli kiritilmagan va kutilmagan tarzda bajarilganda. SQL in'ektsiyasi asosan veb-saytlar uchun hujum vektori sifatida tanilgan, ammo har qanday turdagi SQL ma'lumotlar bazasiga hujum qilish uchun ishlatilishi mumkin.

SQL in'ektsiya hujumlari tajovuzkorlarga identifikatorni buzish, mavjud ma'lumotlarni buzish, tranzaktsiyalarni bekor qilish yoki balanslarni o'zgartirish kabi rad etish muammolarini keltirib chiqarish, tizimdagi barcha ma'lumotlarni to'liq oshkor qilish, ma'lumotlarni yo'q qilish yoki boshqa yo'l bilan mavjud bo'lmasligi va ma'lumotlar bazasi serverining ma'muriga aylanish imkonini beradi. Hujjatga yo'naltirilgan NoSQL ma'lumotlar bazalari ham ushbu xavfsizlik zaifligidan ta'sirlanishi mumkin.

ISSN 2181-3187

4. *Cross-Site Scripting (XSS).* Veb-sahifaga zararli JavaScript kodlarini joylashtirish orqali foydalanuvchilarni aldash yoki ularning hisob ma’lumotlarini o‘g‘irlash. Saytlararo skript (XSS) ba'zi veb-ilovalarda topilishi mumkin bo'lgan xavfsizlik zaifligining bir turi.



XSS hujumlari tajovuzkorlarga boshqa foydalanuvchilar tomonidan ko'riladigan veb-sahifalarga mijoz tomonidagi skriptlarni kiritish imkonini beradi. Saytlararo skriptning zaifligi tajovuzkorlar tomonidan bir xil manba siyosati kabi kirishni boshqarish vositalarini chetlab o'tish uchun ishlatilishi mumkin. 2007 yilning ikkinchi yarmida XSSed Symantec tomonidan hujjatlashtirilgan 2134 "an'anaviy" zaifliklarga nisbatan 11253 ta saytga xos zaifliklarni hujjatlashtirdi. XSS effektlari zaif sayt tomonidan ko'rib chiqiladigan ma'lumotlarning sezgirligiga va sayt egasi tarmog'i tomonidan amalga oshirilgan har qanday xavfsizlikni yumshatish xususiyatiga qarab, kichik noqulaylikdan muhim xavfsizlik xavfigacha o'zgarib turadi.

5. Man-in-the-Middle (MITM) hujumi. Trafikni tutib qolish va manipulyatsiya qilish orqali foydalanuvchi va server o‘rtasidagi ma’lumotlarni o‘g‘irlash.

Kriptografiya va kompyuter xavfsizligida odam-in-the-middle (MITM) hujumi yoki on-path hujumi kiberhujum bo'lib, bunda tajovuzkor bir-biri bilan bevosita aloqada bo'layotganiga ishongan ikki tomon o'rtasidagi aloqani yashirincha uzatadi va ehtimol o'zgartiradi, aslida esa tajovuzkor ikki foydalanuvchi tomoni orasiga kirib qolgan.

MITM hujumining bir misoli faol tinglash bo'lib, bunda tajovuzkor jabrlanuvchilar bilan mustaqil aloqa o'rnatadi va ular o'rtasida shaxsiy aloqa orqali

ISSN 2181-3187

to'g'ridan-to'g'ri bir-biri bilan gaplashayotganiga ishonish uchun xabarlarni uzatadi, aslida esa butun suhbat tajovuzkor tomonidan boshqariladi. Ushbu stsenariyda tajovuzkor ikki qurbon o'rtasida o'tadigan barcha tegishli xabarlarni ushlab turishi va yangilarini kiritishi kerak. Bu ko'p hollarda oddiy; masalan, shifrlanmagan tarmoqqa ega bo'lgan Wi-Fi kirish nuqtasi doirasidagi tajovuzkor o'zini odam sifatida o'rtaga qo'yishi mumkin.

6. Zero-Day hujumlari. Dasturiy ta’minotdagi hali aniqlanmagan va tuzatilmagan zaifliklardan foydalanish orqali amalga oshiriladigan hujumlar.

0-kun (inglizcha *zero day)* - *yamalmagan* zaifliklarni, shuningdek, himoya mexanizmlari hali ishlab chiqilmagan zararli dasturlarni bildiruvchi atama.

Bu atamaning o'zi ishlab chiquvchilarga nuqsonni tuzatish uchun 0 kun vaqt kerakligini anglatadi: zaiflik yoki hujum dasturiy ta'minot ishlab chiqaruvchisi xatoni tuzatishni chiqarishidan oldin ommaga ma'lum bo'ladi (ya'ni, zaiflikdan himoya qilish imkoniyatisiz dasturning ishlaydigan nusxalarida foydalanish mumkin)

7. Ransomware. Kompyuter tizimlarini bloklab qo‘yish yoki ma’lumotlarni shifrlash orqali foydalanuvchidan pul talab qilish.

Ransomware, **shantajchi** (inglizcha *ransomware - ransom* - to'lov va *dasturiy ta'minot* - dasturiy ta'minot so'zlarining ifloslanishi), **winlocker** (inglizcha *winlocker* - Windows blocker)- tovlamachilik uchun mo'ljallangan, kompyuter tizimiga kirishni bloklaydi yoki undan shifrlangan ma'lumotlarni o'qish va undan so'ng shifrlashning asl usullarini oldini oladi davlat.

ISSN 2181-3187

8. API hujumlari. Mijoz ilovalarining ochiq API-laridan foydalanib, noto‘g‘ri so‘rovlar yuborish yoki maxfiy ma’lumotlarga noqonuniy kirish.

API hujumlari - bu zararli yoki ruxsat etilmagan maqsadlarda API-lardan foydalanishga urinishlar. API hujumlari turli shakllarga ega, jumladan:

- API ilovalaridagi texnik zaifliklardan foydalanish
- O'g'irlangan hisob ma'lumotlari va boshqa hisoblarni o'zlashtirish usullaridan qonuniy foydalanuvchi sifatida niqoblash uchun foydalanish
- API-lardan kutilmagan tarzda foydalanishga imkon beruvchi biznes mantig'ini suiiste'mol qilish

9. Session Hijacking (Sessiyani egallash). Foydalanuvchining seans identifikatorini o‘g‘irlash orqali tizimga ruxsatsiz kirish.

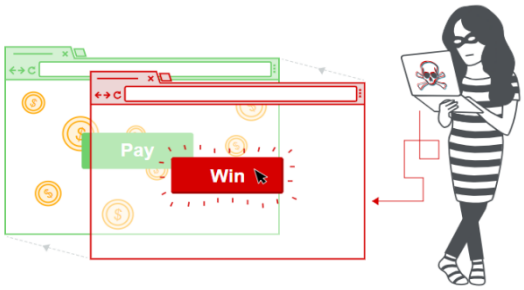
Kompyuter fanida seansni o'g'irlash, ba'zan cookie fayllarini o'g'irlash deb ham ataladi, bu kompyuter tizimidagi ma'lumotlar yoki xizmatlarga ruxsatsiz kirish uchun haqiqiy kompyuter seansidan (ba'zan seans kaliti deb ham ataladi) foydalanishdir.

Xususan, foydalanuvchini masofaviy serverga autentifikatsiya qilish uchun ishlatiladigan sehrli cookie-faylni o'g'irlashga murojaat qilish uchun ishlatiladi. Bu veb-ishlab chiquvchilar uchun alohida ahamiyatga ega, chunki ko'pgina veb-saytlarda sessiyani davom ettirish uchun ishlatiladigan HTTP cookie-fayllari tajovuzkor tomonidan vositachi kompyuter yordamida yoki jabrlanuvchining kompyuterida saqlangan cookie-fayllarga kirish imkoni bilan osongina o'g'irlanishi mumkin (qarang: HTTP cookie-fayllarini o'g'irlash). Tegishli seans cookie-fayllarini muvaffaqiyatli

ISSN 2181-3187

o'g'irlagandan so'ng, raqib seansni o'g'irlashni amalga oshirish uchun Cookie-ni o'tkazish texnikasidan foydalanishi mumkin.

10. Clickjacking. Foydalanuvchini xabar topmagan holda zararli havolalarni bosishga undash orqali tizimga zarar yetkazish.



Clickjacking - bu internet foydalanuvchilarini aldash mexanizmi *bo'lib*, bunda tajovuzkor maxfiy ma'lumotlarga kirishi yoki hatto uni zararsizdek tuyuladigan sahifaga jalb qilish yoki xavfsiz sahifaga zararli kodni kiritish orqali uning kompyuteriga kirish huquqiga ega bo'lishi mumkin. Printsip ko'rinadigan sahifaning tepasiga ko'rinmas qatlam qo'yilishi, unga tajovuzkorga kerak bo'lgan sahifa yuklanishi, kerakli harakatni bajarish uchun zarur bo'lgan boshqaruv elementi (tugmacha, havola) esa foydalanuvchi bosishi kutilayotgan ko'rinadigan havola yoki tugma bilan birlashtirilganligiga asoslanadi. Texnologiya ijtimoiy tarmoq resursiga obuna bo‘lishdan tortib, maxfiy ma’lumotlarni o‘g‘irlash va birovning hisobidan onlayn-do‘konlarda xarid qilishgacha bo‘lgan turli usullarda qo‘llanilishi mumkin.

Foydalanilgan adabiyotlar.

1. Apple Inc., “Face ID: An Introduction,” Apple Developer Documentation, 2017.
2. Lei, Y., & Liu, Z., “Face Recognition Using Deep Learning,” Journal of Machine Learning Research, 2020.
3. OpenCV Documentation, “Face Detection and Recognition,” OpenCV.org, 2021.
4. Sharma, A., & Singh, A., “Biometric Authentication Systems: Challenges and Solutions,” International Journal of Computer Science and Engineering, 2019.